## I claim:

1	1.	An apparatus, comprising:
2		a hash circuit to receive first and second input values for a current hash stage
3		and to generate an output value from the current hash stage based on the
4		first and second input values;
5		a numerical sequencer coupled to the hash circuit to generate a sequence of
6		numbers during the current hash stage and to provide at least a portion
7		of a current one of the sequence of numbers as the first input value for a
8		subsequent hash stage;
9		a feedback circuit coupled to the hash circuit to provide at least a portion of the
10		output value as the second input value for the subsequent hash stage; and
1		a control circuit coupled to the numerical sequencer to stop generating the
12		sequence of numbers upon an occurrence of a first predetermined event
13		and to resume generating the sequence of numbers upon an occurrence
14		of a second predetermined event.
1	2.	The apparatus of claim 1, wherein:
2		the hash circuit is to receive the first and second input values at a beginning of
3		the current hash stage.
1	3.	The apparatus of claim 1, wherein:
2		the first predetermined event includes receipt of a request for a pseudo-random
3		numher

- 1 4. The apparatus of claim 1, wherein:
- 2 the second predetermined event includes a part of the subsequent hash stage.
- 1 5. The apparatus of claim 1, wherein:
- 2 the second predetermined event includes a beginning of the subsequent hash
- 3 stage.
- 1 6. The apparatus of claim 1, wherein:
- 2 The numerical sequencer includes a counter.
- 1 7. The apparatus of claim 1, wherein:
- 2 the numerical sequencer includes a linear feedback shift register.
- The apparatus of claim 1, wherein:
- 2 said at least a portion of the current one of the sequence of numbers includes
- 3 predetermined bits of the current one of the sequence of numbers.
- 1 9. The apparatus of claim 1, wherein:
- 2 said at least a portion of the output value includes predetermined bits of the
- 3 output value.
- 1 10. A system, comprising:
- 2 a processor;
- 3 a memory coupled to the processor; and

2

number.

4		a pseudo-random number generator coupled to the processor and including:
5		a hash circuit to receive first and second input values for a current hash
6		stage and to generate an output value from the current hash stage
7		based on the first and second input values;
8		a numerical sequencer coupled to the hash circuit to generate a sequence
9		of numbers during the current hash stage and to provide at least a
10		portion of a current one of the sequence of numbers as the first
11		input value for a subsequent hash stage;
12		a feedback circuit coupled to the hash circuit to provide at least a portion
13		of the output value as the second input value for the subsequent
14		hash stage; and
15		a control circuit coupled to the numerical sequencer to stop generating
16		the sequence of numbers upon an occurrence of a first
17		predetermined event and to resume generating the sequence of
18		numbers upon an occurrence of a second predetermined event.
1	11.	The system of claim 10, wherein:
2		the hash circuit is to receive the first and second input values at a beginning of
3		the current hash stage.
1	12.	The system of claim 10, wherein:

the first predetermined event includes receipt of a request for a pseudo-random

- 1 13. The system of claim 10, wherein:
- 2 the second predetermined event includes a part of the subsequent hash stage.
- 1 14. The system of claim 10, wherein:
- 2 the second predetermined event includes a beginning of the subsequent hash
- 3 stage.
- 1 15. The system of claim 10, wherein:
- 2 The numerical sequencer includes a counter.
- 16. The system of claim 10, wherein:
- 2 the numerical sequencer includes a linear feedback shift register.
  - 1 17. The system of claim 10, wherein:
- 2 said at least a portion of the current one of the sequence of numbers includes
- 3 predetermined bits of the current one of the sequence of numbers.
- 1 18. The system of claim 10, wherein:
- 2 said at least a portion of the output value includes predetermined bits of the
- 3 output value.
- 1 19. A method, comprising:
- 2 generating a series of values during each of a previous hash stage, a current
- 3 hash stage, and a subsequent hash stage;
- 4 receiving one of the values as a first hash input;

3

- Attorney Docket No. 42390P11973 5 receiving a hash output from the previous hash stage as a second hash input; 6 hashing the first and second hash inputs during a current hash stage to produce a current hash output; 7 stopping the generating when a first predetermined event occurs and restarting the generating when a second predetermined event occurs, if the first predetermined event occurs during the current hash stage; and 10 11 continuing the generating during the current hash stage, if the first 12 predetermined event does not occur during the current hash stage. 20. The method of claim 19, wherein: the first predetermined event includes receiving a request for a pseudo-random 2 3 number. 21. The method of claim 19, wherein: the second predetermined event includes a beginning of the subsequent hash 2
- 1 22. A machine-readable medium having stored thereon instructions, which when executed by at least one processor cause said at least one processor to perform 2
- 3 operations comprising:

stage.

- generating a series of values during each of a previous hash stage, a current 4
- 5 hash stage, and a subsequent hash stage;
- receiving one of the values as a first hash input; 6
- 7 receiving a hash output from the previous hash stage as a second hash input;

8	hashing the first and second hash inputs during a current hash stage to produce a
9	current hash output;
10	stopping the generating when the first predetermined event occurs and restarting
11	the generating when a second predetermined event occurs, if a first
12	predetermined event occurs during the current hash stage; and
13	continuing the generating if the first predetermined event does not occur during
14	the current hash stage.

- 23. The medium of claim 22, wherein:
- the first predetermined event includes a request for a pseudo-random number.
- 24. The medium of claim 22, wherein:
- the second predetermined event includes a beginning of a subsequent hash
  stage.